PKI Technical Working Group

Directory Issues

Ed Reed, Technologist

Novell Product Management

ereed@novell.com

Novell®

Agenda

- **Implications of Wide-Spread Use**
- **Namespace Integration Requirements**
- **The Politics of Data Ownership**
- **Q & A**

Novell®

Implications of Wide-Spread Use

Novell®

There’s a vast range of Uses

- **Identity and Relationship Modeling**
- **Address Books, Certificate Servers**
- **Network Registry and Name Services**
- **Configuration of Services and Devices**
- **Policy and Access Controls for Applications and Services**

Novell®

Each with their own Preferences

- **Protocols and APIs**
- **Data access patterns**
- **Namespace shapes and sizes**
- **Schema and Data Integrity**
- **Control and Delegation**

Innovation Drives Differentiation

- **There'll Never be just one**
  - **Top level domains**
    - **DNS, X.500, LDAP, Bi-lateral agreements**
  - **Protocols (DNS, LDAP, X.500, …)**
  - **Administrative Authorities**
    - **Global, Enterprise, Departmental, Consumers, Application Data Owners**
  - **Trust models**

Novell®

So, Wide Spread Use Means…

- **Flexibility will be paramount**
  - **Configuration and Deployment choices**
  - **Expect Heterogeneous Namespaces**
  - **Design Homogeneity out of existence**

Namespace Integration Requirements

Novell®

LDAP Apps Must Be Distributed Apps

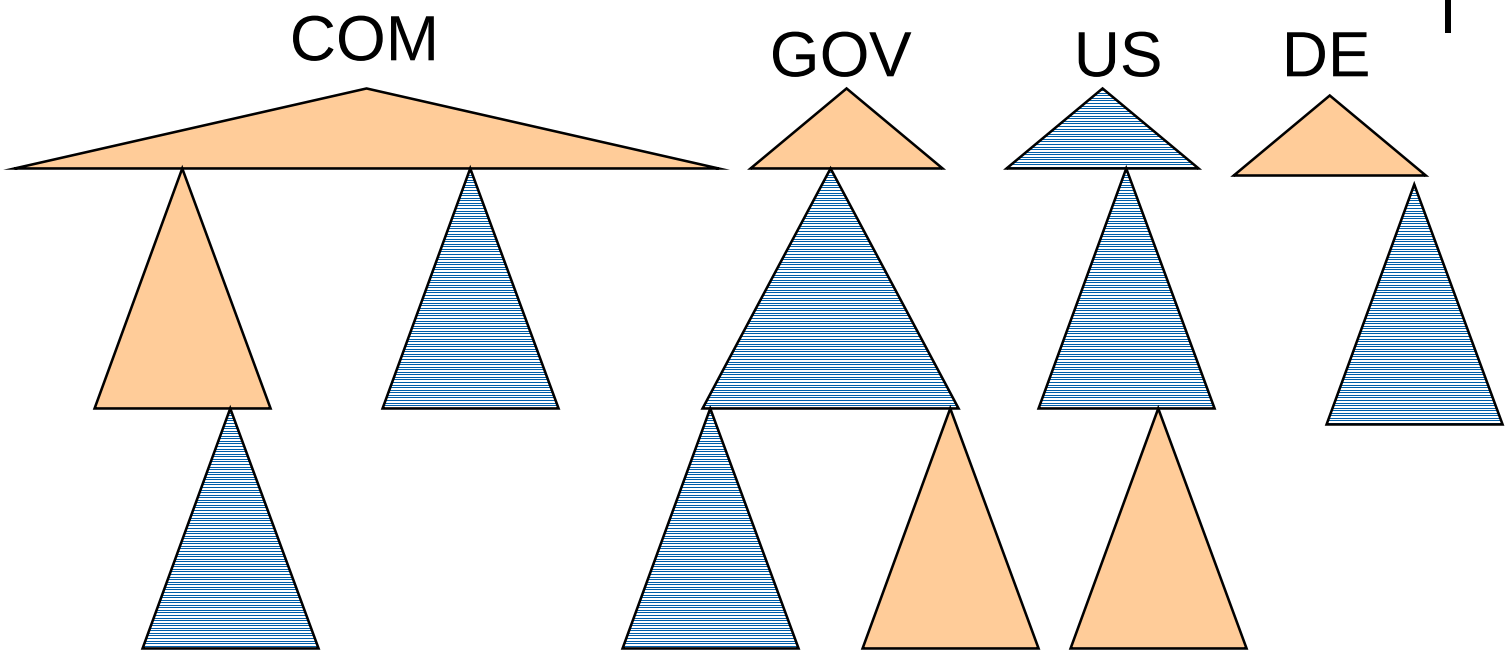
- **LDAPv3 clients are imperative**
  - **referral chasing is a short term solution**
- **LDAP chaining (ala DSP) is also imperative**
  - **For stupid (sorry, LDAPv2) clients**
  - **For fire-walled services**
  - **To traverse foreign namespaces**

And further more...

- **LDAP namespace federation via DNS is imperative**
  - **Server-based resolve-name facilitates**
  - **Trust achieved via authentication, not name subordination**
  - **DNSSEC required for widespread use**
  - **Never-mind the organizational vs geographical naming battles!**

Novell®

Namespace Federation



DNS Namespaces

LDAP & X.500 Namespaces

Naming is a political issue, not a technical one

Novell

Heterogeneous Namespaces Are Nothing New

- **Client-side Federation via APIs**
  - **XFN, JDSI, even ADSI!**
  - **Clients parse names, handle multiple protocols**
- **Server-side Resolve Name (Chaining)**
  - **Use Available Distributed Knowledge**
    - **Use SOA, NS, A, PTR for DNS**
    - **Subordinate References for X.500 & NDS**
    - **LDUP Subentries and LDAP Knowledge Referrals**
  - **Return Referrals as appropriate**

Novell®

The Politics of Data Ownership

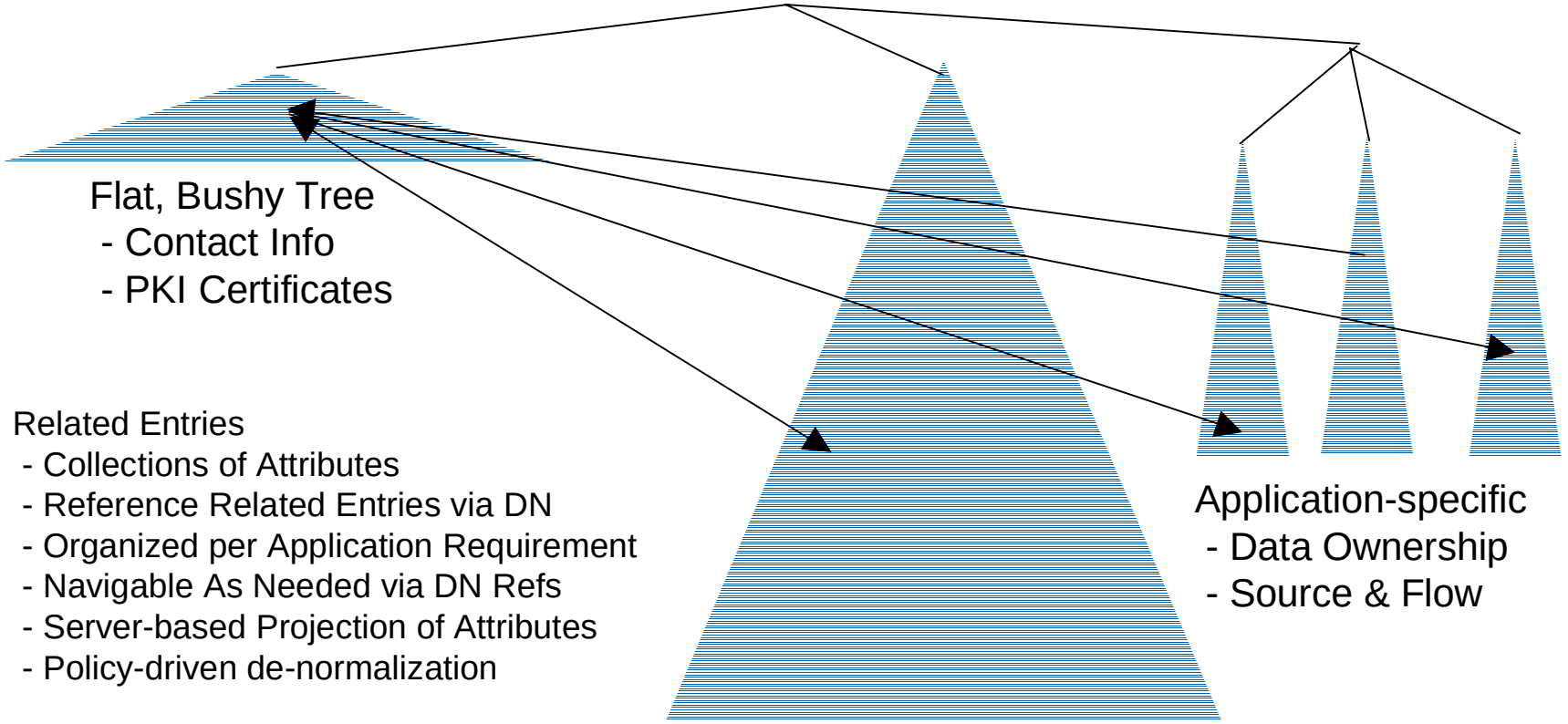
Novell®

The Politics of Data Ownership

- **No Single Hierarchy Is Sufficient**
- **Application-Specific Policies**
  - **Access Control, Inheritance**
  - **Data Ownership**
  - **Direction of Change Notification**
- **Data Access Patterns**
  - **Search**
  - **Lookup**
  - **Browse**

Novell®

Entries Related Via Policy, Data De-normalized As Needed



Flat, Bushy Tree
- Contact Info
- PKI Certificates

Related Entries
- Collections of Attributes
- Reference Related Entries via DN
- Organized per Application Requirement
- Navigable As Needed via DN Refs
- Server-based Projection of Attributes
- Policy-driven de-normalization

Application-specific
- Data Ownership
- Source & Flow

Rich, Deep Tree
- Operational
- Organizational

Novell®

Key Messages

- **No singly indexed database application has ever been generally useful - and the directory isn’t the first**
- **Single entries and their ACLs don’t make it easy to allow data owners to own their data**
- **Server-based, policy constrained, selective de-normalization of attributes among related entries is required**

Novell®

Directory Interoperability Forum

News Flash

7 July 1999

Novell®

Directory Interoperability Forum

- **IBM, Novell, Lotus, Oracle, DCL, Isocor + 30 ISV supporters**
- **Close ties with The Open Group**
  - **Directory Certification Program**
  - **Application Certification Program**
- **Web Site: http://www.directoryforum.org**

Novell®

Q & A

Novell®